PLAN DE SEGURIDAD Y TRATAMIENTO DE RIESGOS DE LA INFORMACION
VIGENCIA 2026

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES SEGUNDO TRIMESTRE	RESPONSABLE
				1	2	3	4	1	2	3	4		
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	Capacitar al personal de la institucion en la toma de conciencia y actualizacion regular en las políticas de seguridad de la información y procedimientos relacionados a su cargo.	Capacitación en seguridad de la información.	1	1	1	1	1	1			Se llevó a cabo jornada de capacitación en seguridad informática y uso eficiente de los recursos tecnológicos, dirigidas al personal de las diferentes áreas del Sanatorio.	Talento Humano y Sistemas
		Establecer, documentar y revisar una política de control de acceso con base en los requisitos de seguridad de la información.	Documentar política de control de acceso implementada.	50%	50%	100%	100%	15%	20%			No se ha documentado la política de control de acceso	Talento Humano y Sistemas
		Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Copias de seguridad.			100%	100%	_	25%			Se realizan copias de seguridad de la página web y la plataforma de datos GD, y se inicializan las copias de algunas cuentas de correo.	Sistemas
		Identificar los cambios en la organización, en los procesos de sistemas, procesamiento de información que afectan la seguridad de la información.	Análisis de cambios realizados / Cambios presentados en el periodo	100%	100%	100%	100%	0%	25%			Se realizó una solicitud al soporte de GD referente a los procesos de facturación, con el objetivo de mejorar las áreas de cartera y urgencias.	Sistemas
		Implementar controles de prevención, de detección y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Procedimiento implementado	100%	100%	100%	100%	100%	100%			Se mantiene un monitoreo continuo por parte del equipo CSIRT en la red del sanatorio, con el objetivo de detectar posibles anomalías, prevenir incidentes de seguridad y proteger la información.	Sistemas
		Implementar procedimientos para controlar la instalación de software en sistemas operativos.	Procedimiento documentado e implementado	100%	100%	100%	100%	45%	0%			Pendiente documentar el procedimiento	Sistemas